Barracuda Networks Technical Documentation

Barracuda NG Firewall

Release and Migration Notes

Version 5.0.3

RECLAIM YOUR NETWORK™

Copyright Notice

Trademarks

Content

General

Warning

Read this document **before** updating your system

Caution

If you are going to update from **release version 4.2** to Barracuda NG Firewall 5.0.3, Barracuda Networks strongly recommends to study the Barracuda NG Firewall 5.0 Migration Instructions available for download at **http://barracuda.com/doc**, as, under certain circumstances, no countermanding is possible once the updating process was initiated.

For in-depth information about new features and changes in terminology introduced with release version 5.0, please refer to the **Barracuda NG Firewall 5.0 Migration Instructions** downloadable from the same source.

Caution

Starting with Barracuda NG Firewall 4.2.13, OVA images for VMWare were made available. OVA images based on minor release 4.2.13 have a bug which might lead to loss of the current network configuration when updating to Barracuda NG Firewall minor release 5.0.3.
Please make sure to configure your network settings **before updating** virtual appliances based on 4.2.13 OVA images using Barracuda NG Admin at least once. Also, a network activation is required.
This issue does not apply to fresh installations based on 5.0.3 OVA images.

Note

The Barracuda NG Firewall may reboot after installation. If not, Barracuda Networks recommends performing a manual reboot.

GPL Compliance Statement

This product is in part Linux based and contains both Barracuda Networks proprietary software components and open source components in modified and unmodified form. A certain number of the included open source components underlie the GPL or LGPL or other similar license conditions that require the respective modified or unmodified source code to be made freely available to the general public, this source code is available on http://source.barracuda.com.
Please also refer to the chapter ***Warranty ans Software License Agreement*** of the Barracuda NG Firewall 5.0.3 Administrator's Guide documentation located in the documentation section on www.barracuda.com and on each accompanying USB thumb drive.

Supported Hardware

Table 1–1 Barracuda Networks Appliances Supported By Barracuda NG Firewall 5.0.3

Barracuda Networks Appliances Supported by Barracuda NG Firewall 5.0.3
Hardware Appliances: F10, F15, F100, F200, F300, C400, C610, F400, F600, F800, F900
Virtual Appliances: VC400, VC610, VC820
Standard Hardware: Please consult the Barracuda Networks Technical Support for information on Barracuda NG Firewall 5.0.3 on standard hardware..

Minimum System Requirements

Caution

If you are going to upgrade standard hardware or phion netfence hardware to Barracuda NG Firewall 5.0.3, please ensure that at least **2 GB of free storage space** is available on the root partition. If this minimum amount of space is not available, Barracuda Networks highly recommends to re-install the system with a larger root partition instead of upgrading. On appliances with hard disk, the upgrade package requires additionally **another 2 GB** of free storage space on the `/phion0` partition for storing temporary data. This additional space is not necessary on Flash based appliances.

Table 1–2 Minimum system requirements for Barracuda NG Firewall

Operation System	included (Barracuda OS)
Disk space	15 GB on a dedicated harddisk for gateway installation on harddisks 4 GB for gateway installation on a CF flash card with 1.5 GB of free space 30 GB on a dedicated harddisk for Barracuda NG Control Center installation 2 GB of free storage space on the root partition 2 GB of free storage space on the `/phion0` partition 50 MB of free storage space on the `/boot` partition.
RAM	512 MB
Processor	400 MHz, i686 compatible The CPU must support the TSC and CMOV instructions. Installing or updating systems with older CPUs will exit with an error.
Networking	1 network interface required
Partitioned space	The boot partition must have a size of at least 50 MB. Updating a system with a smaller boot partition size exits with an error. Therefore, Barracuda Networks recommends to perform a fresh installation instead of updating, as with a fresh installation the partition size will automatically be adjusted correctly.

Table 1–3 Minimum system requirements for Barracuda NG Admin / Barracuda NG Installer

Operation Systems	Windows XP, Windows Vista (32-bit, 64-bit), Windows 7 (32-bit, 64-bit) with Microsoft .NET Framework 3.5 SP1 **or** Microsoft .NET Framework 4.0 **or** later
Disk space	30 MB
RAM	1 GB
Processor	1 GHz

Known Issues

Note

Advice about known issues is available at **www.barracuda.com** or through the Barracuda Networks support.

If you are using standard hardware and / or updating from phion netfence, please pay also attention to the ***Barracuda NG Firewall 5.0 Migration Instructions*** and the ***Barracuda NG Firewall 5.2 Migration Instructions*** available for download at **http://barracuda.com/doc**, as in this case numerous known issues and hardware restrictions will apply.

Updates with Firmware 5.0 Minor Release 3

Update Matrix

Table 1–4 Update matrix - supported and not supported update cases

		Target Version			
		5.0	**5.0.1**	**5.0.2**	**5.0.3**
Current Version	4.2.10 and earlier	-	-	-	-
	4.2.11	✓	✓	✓	✓
	4.2.13	✓	✓	✓	✓
	4.2.14	✓	✓	✓	✓
	4.2.15	✓	✓	✓	✓
	4.2.16	✓	✓	✓	✓
	5.0	-	✓	✓	✓
	5.0.1	-	-	✓	✓
	5.0.2	-	-	-	✓

Note

If you are going to update from a firmware release version below 5.0, then please see the ***Barracuda NG Firewall 5.0 Migration Instructions*** (published together with major release 5.0) available as a separate document at **http://barracuda.com/doc** before executing the update.

Software Modules and Components Affected by Minor Release 5.0.3

Table 1–5 Affected Software Modules and Components

		Affected by Minor Release		
		5.0.1	5.0.2	5.0.3
Software Modules	Firewall	✓	✓	✓
	VPN Service	✓	✓	✓
	Access Control Service	✓	✓	-
	HTTP Proxy	✓	✓	✓
	Secure Web Proxy	✓	-	-
	URL Filter	✓	✓	-
	Mail Gateway	✓	-	✓
	Spam Filter	-	-	-
	Virus Scanner	✓	-	-
	DHCP Service	-	✓	-
	DHCP Relay	-	-	-
	DNS	-	-	-
	FW Audit Log Service	✓	-	-
	FTP Gateway	✓	✓	-
	OSPF/RIP Service	-	-	-
	SNMP Service	✓	-	✓
	SSH Proxy	-	✓	-
	Authentication	-	✓	✓
	Statistics	-	✓	-
Other	Barracuda OS	✓	✓	✓
	NG Control Center	✓	✓	✓
	Network	✓	✓	✓
	NG Admin	✓	✓	✓
	NG Installer	✓	✓	✓
	NG Network Access Client	✓	✓	-
	VPN Client R8 for Mac	-	✓	-

Bugfixes Included with Barracuda NG Firewall 5.0.3

Barracuda NG Admin

Table 1–6 Barracuda NG Admin

Description
Within the ***Network Interface Configuration***, pop-ups erroneously appeared every time after changing the ***Appliance Sub Model Type*** in a VLAN interface. This issue was fixed.
In rare cases, the ***Send Changes*** button was erroneously disabled within the ***Personal Firewall Rules Configuration***. This issue was fixed.
Updating two units within two different tabs in Barracuda NG Admin at the same time resulted in failing update procedures. This issue was fixed.

Barracuda NG Installer

Table 1–7 Barracuda NG Installer

Description
Barracuda NG Installer was for virtual appliances in some cases erroneously not setting the model version as intended, leading to configuration problems in Barracuda NG Admin subsequent to the installation process. This issue was fixed.
Barracuda NG Installer failed to execute automated USB thumb drive installations on flash-based appliances if there were additional USB devices connected to the appliance. The following error message was generated: `An error occurred finding the installation image on your hard drive. Please check your images and try again.` This issue was fixed.

Barracuda NG Firewall

Table 1–8 Barracuda NG Firewall

Module	Description
Authentication	Occasionally, a few log lines were missing in the authentication log. This issue was fixed.
Authentication	Occasionally, the firewall authentication daemon was erroneously blocking requests if these requests were sent delayed by the respective clients. This issue was fixed.
Authentication	Active Directory offline group synchronization was erroneously not using SSL even when it was configured to use it. This issue was fixed.
Barracuda OS	HDD performance I/O statistics were erroneously not logged. This issue was fixed
Barracuda OS	An issue within the VPN Client-to-Site and SSL VPN NAC licenses prevented these licenses from being correctly recognized on VF1000 (and probably also other Vxxxx) virtual appliances. This issue was fixed.
Barracuda OS	On VF250 virtual machines, it could erroneously happen that P2P detection generated an error stating that the license for P2P detection was limited to 100 units, although the license was not limited to this value. This issue was fixed.
Firewall	Big amounts of global firewall objects were, even if they were not referenced in a ruleset, leading to high memory consumption. This issue was fixed.

Table 1–8 Barracuda NG Firewall

Module	Description
Firewall	The detection of large packet sizes (PMTU discovery) did not work in conjunction with local redirection rules. This issue was fixed.
HTTP Proxy	Infrequently, the Proxy GUI in Barracuda NG Admin was not fed anymore with up-to-date status information due to an issue within the HTTP Proxy module. This issue was fixed.
Mail Gateway	Due to a database problem, the Mail Gateway erroneously went down on rare occasions and had to be restarted manually. This issue was fixed.
Network	On VFxxx virtual machines, it was erroneously not possible to select previously configured additional interfaces directly after the virtual machine was installed. This issue was fixed.
Network	The authentication daemon erroneously crashed when a device tried to authenticate while at the same time leaving the WiFi's transmission range. This issue was fixed.
Network	The activation of bonding on a unit could under certain circumstances result in the creation of erroneous MAC mapping tables. This issue was fixed.
Network	An erroneous match for the priority of a 3G or xDSL routing rule caused previously assigned source addresses to remain part of the source match condition, which was leading to the creation of a stack of rules that eventually exhausted the maximum number of rules. This issue was fixed.
Network	The IP address for a DHCP link that had been configured to use Dynamic DNS was erroneously not updated as intended. This issue was fixed.
NG Control Center	In conjunction with different firmware release versions on a Barracuda NG Control Center and its managed units, certain configuration options may erroneously have been unavailable on the NG Control Center, such as e.g. URL filter categories for a 4.2.x cluster on a 5.x NG CC. This issue was fixed.
NG Control Center	It was erroneously not possible to add a WLAN node to the Repository. Any attempt to do so failed with an error pop-up message saying `Copy to Repository Status: Error`. This issue was fixed.
NG Control Center	In very rare occasions and only in conjunction with different release versions on an NG CC and its managed units, Barracuda NG Control Center assigned erroneous default NIC driver names to certain managed units. This issue was fixed.
NG Control Center	Under certain circumstances, Repository directories could erroneously get wrong label names after a migration process. This issue was fixed.
SNMP Service	Blocked services were through SNMP erroneously indicated as being started. This issue was fixed.
VPN Service	At very rare occasions, the internet key exchange (IKE) service crashed, resulting in a short service interruption with currently open VPN tunnels, as these tunnels went down and were then automatically re-created.
VPN Service	NAT traversal did erroneously not work with site-to-site tunnels. This issue was fixed.
VPN Service	Terminating VPN tunnels via Barracuda NG Admin was on rare occasions leading to a kernel panic. The same problem could also occur in conjunction with Access Control Service connections on certain ports. This issue was fixed.
VPN Service	The VPN Service occasionally crashed with certificates that contained long subject names. This issue was fixed.

Determine Your Update Scenario

Caution

If you are going to update **firmware version 4.2** to Barracuda NG Firewall 5.0.3, Barracuda Networks strongly recommends to study the instructions given in this chapter, as, under certain circumstances, no countermanding is possible once the updating process was initiated.

Note

Updating to Barracuda NG Firewall minor release 5.0.3 is only possible from release versions 4.2.x, 5.0, 5.0.1, or 5.0.2. Direct updating from release versions 4.0.x or 3.x is not possible. Update to 4.2 first.

To update from firmware 4.2.x, use the `update.[xxx].tgz` file.
To update from firmware 5.0.X, use the `patch.[xxx].tgz` file.
For a fresh installation, use the `*.iso` file.

Note

In case you are updating a HA synchronized unit to firmware release version 5.0.3 while not updating its secondary unit as well, or vice versa, so that the units run on different firmware versions, it may be necessary to re-synchronize the units after updating. To do so, click ***Firewall > Live > Show Proc***, select the process named ***Sync Handler*** and choose ***Kill Selected***. Session synchronization will automatically re-appear subsequently.

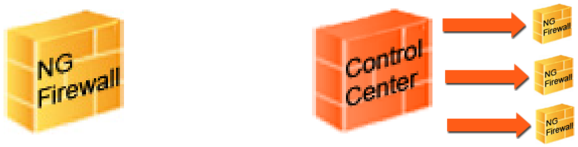
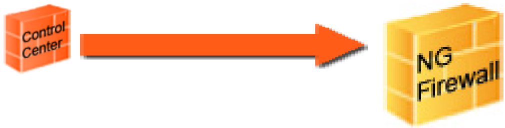
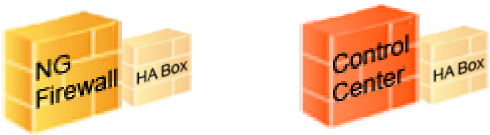
Note

For the reason of updating speed, updating via the ***Firmware Update...*** button in Barracuda NG Admin is not recommended. This is especially valid for slow hardware or the flash based appliances F10, F100 or F101, although it is possible. Barracuda Networks strongly recommends to perform the updating process using SSH as described above.

Before beginning the updating process, you should clarify which types of hardware and administrative configuration you have.

Barracuda NG Firewall 5.0.3 and its predecessors allow different administrative configurations. Please follow those update instructions that apply to your configuration

Table 2–9 Different Administrative Configurations

Administrative Configuration Type	Applicable Update Instructions
Unmanaged Unit or NG Control Center  NG Firewall Control Center NG Firewall NG Firewall NG Firewall	If you want to update either **an unmanaged unit or an NG Control Center**, then proceed to *Updating Unmanaged Units or NG Control Centers, page 15*.
NG Control Center Managed Unit  	If you want to update **a unit that is managed by an NG Control Center**. then proceed to *Updating NG Control Center Managed Units, page 18*.
Unit or NG Control Center  **Combined with HA Unit**	If you want to update **a unit or an NG Control Center** that is **combined with a High Availability (HA) unit**, then proceed to *Updating HA-Synced Units or HA-Synced NG Control Centers, page 16*.

Updating Unmanaged Units or NG Control Centers

Updating Units or NG Control Centers Using SSH

Best Practice

For speed reasons, Barracuda Networks recommends using this method of updating for all appliances in general, especially for those based on a flash drive or slower hardware.

Step 1: Copy

Before copying the package onto the unit as described below, make sure that there is no old minor release or patch package lurking within the `/var/phion/packages/` directory. The directory must not contain any files.

Although the `/var/phion/packages/` directory must be empty, it still contains the subdirectories: `kl, os, ph, sa, tgz.` These don't affect the updating process. Furthermore, there must not be a whitespace character within path or file name of the package.

- ***Copy the update package onto your firewall system into the*** `/var/phion/packages/` ***directory of the respective unit.***

To get the file onto the unit, you may use the ***Send File*** button within the built-in SSH client of Barracuda NG Admin. Don't forget to change the directory first using `cd /var/phion/packages/.`

Step 2: Update

Start the update sequence by executing `phionUpdate` from the shell.

No more interaction is necessary. Wait until the update is finished. Depending on the hardware, it will need from 15 minutes on the fastest appliances up to 60 minutes on the flash appliances.

Warning

Do not interrupt the update procedure. During update, the unit boots several times and due to this, the connection will be terminated. Whether the update process has been successfully finished is confirmed by output on the console, log messages, and firmware version and status displayed within ***Control > Licenses.***

Updating HA-Synced Units or HA-Synced NG Control Centers

In the instructions below, the term "primary unit" refers to the unit used for regular operation, while "HA unit" refers to the secondary unit used as a failover system.

Caution

For Firewall and Configuration HA synchronizing, the primary and the HA unit must both run at least firmware release versions between 4.2.11 and 5.0.3.

Barracuda Networks strongly recommends to follow the procedure for updating HA systems exactly as described below in order to minimize any operational drop outs.

Step 1: Prepare the HA Unit

- ***Log-in to the HA unit using Barracuda NG Admin.***
- ***Block the (standby) server on the HA unit within** Control > Server**.***

Step 2: Update the HA Unit

- ***Update the HA unit using SSH as delineated in** Updating Units or NG Control Centers Using SSH, page 15**.***

No more interaction with the HA unit is necessary. Wait until the update is finished. Depending on the hardware, it will need from 15 minutes on the fastest appliances up to 60 minutes on the flash appliances.

Warning

Do not interrupt the update procedure. During update, the unit boots several times and due to this, the connection will be terminated. Indicators that the update process has been finished are the following output on the console: `Barracuda NG Firewall release 5.0.3-xxx`, or the operativeness of logging in again using SSH or Barracuda NG Admin.

Step 3: Switch Servers to the HA Unit and Prepare the Primary Unit

- ***Log-in to the primary unit using Barracuda NG Admin.***

Proceed after having assured that the HA unit is fully functional.

- ***Unblock the (standby) servers on the HA unit by clicking Stop Server within Control > Servers.***

- ***Log-in to the primary unit using Barracuda NG Admin.***

- ***Switch all servers from the primary to the HA unit and verify for correct operability. Therefore, Block all Servers on the primary unit.***

You may leave the primary unit in standby mode until correct operability of the HA unit has been verified. Click ***Stop Server*** on the primary unit in order to achieve this. If functional errors occur on the HA unit, you may switch servers back to the primary unit.

Step 4: Update the Primary Unit

- ***Update the primary unit using SSH as delineated above in Updating Units or NG Control Centers Using SSH, page 15.***

No more interaction with the primary unit is necessary. Wait until the update is finished. Depending on the hardware, it will need from 15 minutes on the fastest appliances up to 60 minutes on the flash appliances.

Warning

Do not interrupt the update procedure. During update, the unit boots several times and due to this, the connection will be terminated. Indicators that the update process has been finished are the following output on the console: `Barracuda NG Firewall release 5.0.3-xxx`, or the operativeness of logging in again using SSH or Barracuda NG Admin.

Step 5: Switch Servers Back to the Primary Unit

- ***Log-in to the respective primary unit using Barracuda NG Admin.***

Proceed after having assured that the primary unit is fully functional.

- ***Re-enable all servers on the primary unit by clicking Stop Server (Control > Server) on each.***

- ***Log-in to the HA unit using Barracuda NG Admin.***

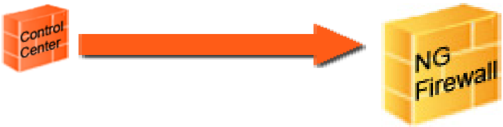
- ***Block all the servers on the HA unit by clicking Block Server (Control > Server).***

Proceed after having assured that the primary unit is fully functional.

- ***Set all the servers on the HA unit back to standby by clicking Stop Server (Control > Server).***

The update process is finished.

Updating NG Control Center Managed Units



To make use of the multi-release capabilities of Barracuda NG Control Center, all units within one cluster must run under the same software major release version. Migration of the NG CC configuration is only available for all units, servers and services of a cluster simultaneously.

Step 1: Import the Update Package into the NG Control Center

- ***Log-in to the Barracuda NG Control Center using Barracuda NG Admin.***
- ***Navigate to Control > Firmware Update and click Import...***
- ***Select the update package within the file browser.***

Step 2: Select Units to Update and Send them the Update

- ***Choose the desired Range, Cluster or Box.***
- ***Select the previously copied update within the Files list.***
- ***Click Create Task...***
- ***Choose Immediate Execution from the Scheduling drop-down menu and click OK.***

Step 3: Execute the Copied Update

- **Navigate to *Control > Update Tasks.***
- ***Verify if the update package was successfully copied, which is indicated by a green icon within the Σ column.***
- ***Right-click the desired unit and select Perform Update followed by Immediate Execution from the Schedule dropdown menu.***

No more interaction with the unit is necessary. Wait until the update is finished. Depending on the hardware, it will need from 15 minutes on the fastest appliances up to 60 minutes on the flash appliances.

Note

Take a look into the box log file at ***Box > Logs >*** `Box\Release\update` after the update process has been finished. In case of a not succeeded update please consult `Box\Release\update_hotfix` for a detailed log.

Note that when updating a unit, the migration is executed at unit level and not on the Barracuda NG Control Center itself.

Migrating from phion netfence to Barracuda NG Firewall 5.0.3

Release version 5.0 of Barracuda NG Firewall was a switchpoint for customers that have been using phion netfence before. With release 5.0, phion netfence was replaced by Barracuda NG Firewall.

Apart from the new features and a new interface design, the usage concepts and system architecture stay the same.

Caution

If you are migrating from phion netfence 4.2.x to Barracuda NG Firewall 5.0.3 on **standard hardware**, you need to **apply hotfix 386 before migrating from 4.2.x to 5.0.3** in order to make use of the MAC-to-eth mapping feature that will help you to keep the port labeling as it is.
Please see ***Updating Standard Hardware from 4.2.x to 5.0.3***, page 21, in this case.

Please consult the Barracuda Networks Technical Support for in-depth information on the migration process on certain standard hardware.

Default Management IP Address and Default Password

Note that, already with release version 4.2, the default management IP address for all Barracuda NG Firewall appliances, NG Control Centers and Virtual Appliances was changed to `192.168.200.200`. However, on legacy phion appliances and phion management centres, the management IP address didn’t change.

The default root password, no matter which hardware is used, was at the same time changed to `ngf1r3wall`

Related Docs

See the ***Barracuda NG Firewall 5.0 Release Notes*** to learn more about the new features introduced with major release version 5.0 and the ***Barracuda NG Firewall 5.0 Migration Instructions*** to learn about all important issues appearing when updating from release version 4.2 to release version 5.0.
Both documents are available at **http://barracuda.com/doc**.

Related Docs

See the appropriate ***Appliance Installation Guide*** or the ***Quick Installation Guide*** for your appliance to learn more about the default settings. The latest documentation is always available at **http://barracuda.com/doc** .

Issues and Restrictions when Updating from phion netfence

Related Docs

For a detailed list of known issues and hardware restrictions appearing when updating from phion netfence to major release version 5.0 please see the ***Barracuda NG Firewall 5.0 Migration Instructions***, downloadable at **http://barracuda.com/doc**.

Updating Standard Hardware from 4.2.x to 5.0.3

General

Due to a kernel version change between 4.2.x and 5.0.3 (Linux kernel 2.4 was changed to Linux kernel 2.6), the enumeration of NICs may on some hardware sort the ethX devices in a different order, resulting in a loss of management access.

Therefore, a procedure has now been implemented to rename the interfaces after upgrading to 5.0.3 to stay identically with the 4.2.x interface names. This is done by creating an interface mapping table using the eth device's MAC addresses as identifiers.

The following procedure **must be performed on every single unit separately** due to the fact the MAC addresses are different per unit and so will be the mapping table.

If you find out later that your server is not affected by the resorting issue, then you may delete the mapping configuration subsequently. The network activation log will then contain the following message:

```
No difference found between configured and detected MAC to interface mapping
```

- ***Update is possible on standalone as well as on NG CC-managed units from firmware 4.2.0 onwards to 5.0.3.***
- ***Updating from a base release in the range from 4.2.0 to 4.2.14 requires a hotfix to be installed. 4.2.15 and 4.2.16 include the functionality, hence no hotfix is required.***
- ***It is recommended to evaluate the process on a system with physical access or in a lab environment in case the upgrade fails.***
- ***The procedure is compatible with user defined interface mappings. If a user defined interface mapping is found, it will be applied after the MAC-to-eth mapping procedure.***
- ***If you add additional NICs after upgrading to 5.0.3, the mapping may fail. Therefore, do not use MAC mapping in this case any longer but switch to user defined interface mapping. The problem may occur if linux detects the new NICs before it detects the old ones.***

Updating Procedure

Step 1: Prepare the Standard Hardware For the Update

- ***If the unit runs on firmware 4.2.14 or below, you must install the hotfix*** `boxnet_mac2ifmapping-386-4.2.14`*.*

Step 2: Generate the Mapping Data

- ***Log-in to the unit via ssh as root and issue the following command:***
  `CreateMACMapping`
  Running this program multiple times will do no harm.

- ***Copy the output lines of the program beginning with*** `CM` ***and those beginning with*** `CI` ***to the clipboard.***

Step 3: Apply the Mapping Data

- ***On standalone units, open the Box Network Configuration within Barracuda NG Admin.***
  On NG CC-managed units, open the Box Network Configuration within Barracuda NG Admin on the respective Barracuda NG Control Center.

- ***Paste the content of the clipboard to Network > Interfaces > MAC Mapping (only visible in Advanced configuration mode).***

- ***Set Use Assignment to yes.***

- ***Click Send Changes followed by Activate.***

Step 4: Proceed to the Update

- ***Upgrade the unit following the standard 5.0.3 upgrade procedure as described in Determine Your Update Scenario, page 13.***

When the update process is finished, please verify if all interfaces are correctly mapped.

Note

In case the linux kernel 2.4 assigned the interfaces in the same order as the linux kernel 2.6 did, the following message will be generated into the 5.0.x box network activation log:

```
No difference found between configured and detected MAC to interface mapping
```

In this case you may disable MAC mapping. This will make the configuration hardware-independent, providing you with more flexibility in case hardware will be changed somewhen in the future.

Note

Further advice about updating standard hardware is available through the Barracuda Networks support.

Barracuda Networks Technical Documentation

RECLAIM YOUR NETWORK™